FindExecutableImage

Return value buffer must be large enough to hold returned path

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4959 bytes

Attack Category	• Path spoofing or confusion problem • Malicious Input
Vulnerability Category	• Buffer Overflow • Threading and synchronization problem • Indeterminate File/Path • Input source (not really attack) • Unconditional
Software Context	• File Management
Location	• dbghelp.h orimagehlp.h
Description	The FindExecutableImage function locates an executable file. The buffer used to return the executable file's name must be large enough to hold the returned value. Note: All DbgHelp functions, such as this one, are single threaded. Therefore, calls from more than one thread to this function will likely result in unexpected behavior or memory corruption. To avoid this, you must synchronize all concurrent calls from more than one thread to this function.
APIs	**Function Name** / **Comments** FindExecutableImage FindExecutableImageEx
Method of Attack	If an attacker can get this program to locate an executable whose full path longer than the file-path buffer, a buffer overflow can occur.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** This solution is always applicable. / The developer MUST ensure that the ImageFilePath / This solution will remove the threat of buffer overflows.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

		is defined large enough to hold the result. The best way to do this is to make sure the buffer is initialized to a length of MAX_PATH + 1. Check that the return buffer is still null terminated.	

Signature Details	HANDLE FindExecutableImage(PCSTR FileName,PCSTR SymbolPath,PSTR ImageFilePath);

Examples of Incorrect Code	`/* Improper buffer allocation for ImageFilePath argument`
	`* FileName and SymbolPath are already specified */`
	
	`PSTR ImageFilePath [20]; //What happens if the file path is longer than 20? Buffer overflow:`
	`FindExecutableImage(FileName, SymbolPath, ImageFilePath);`

Examples of Corrected Code	`/* Improper buffer allocation for ImageFilePath argument`
	`* FileName and SymbolPath are already specified */`
	
	`PSTR ImageFilePath [MAX_PATH + 1]; //The OS will not return a file path longer than this`
	`if (FindExecutableImage(FileName, SymbolPath, ImageFilePath) == NULL)`
	`return false; //Handle any error that may occur.`

Source Reference	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/findexecutableimage.asp[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com